Partner has sent a new IBAN: how to avoid a fraudulent payment?

For: Paušalni obrt · Obrtnici · j.d.o.o. · d.o.o. · Privatni iznajmljivač · Platformski radnik kod poslodavca · Platformski rad preko vlastitog obrta

Practical business guidance · Reviewed: 2026-11-16

Applicability: Practical application according to the circumstances of the business

Please confirm any changes to your payment details by another, already established communication channel before making the payment.

What does that mean in practice?

The sender's name is not proof of identity. An attacker can use a similar domain or have taken over an actual collaborator's account.

Establish a simple internal rule: changes to payment accounts are not confirmed by replying to the same message alone.

An example from everyday business

The associate requests payment to a different account and emphasises the urgency. The entrepreneur first calls the previously saved number and only after verification proceeds with the payment.

Specific next steps

1. Hold the urgent payment until you have verified the request.
2. Call a contact you already have, not the number from the suspicious message.
3. Record the confirmation and the change in the business records.

Most common mistakes

• Only check the logo in the signature.

• Reply only to the same suspicious sender.

Limits of application

Editorial business guideline. The example is illustrative; it is not a legal, tax or accounting calculation.

Sources

CERT.hr · resilience to cyber-attacks

https://www.cert.hr/savjeti-za-povecanje-otpornosti-na-kiberneticke-napade/

Original page

https://adriatrends.hr/poslovni-vodic/en/pitanja/lazni-racun-promjena-iban